CS 5430

Goals and Requirements

Prof. Clarkson
Spring 2017

Review

- **Aspects of security:** confidentiality, integrity, availability
- **Concepts:** Harm, threat, vulnerability, attack, countermeasure
- **Principles:** Accountability, least privilege, defense in depth, open design, ...

Today: system-specific security goals

Engineering methodology

1. Functional requirements
2. Threat analysis
3. Harm analysis
4. Security goals
5. Feasibility analysis
6. Security requirements

1. Functional requirements

- Security = **does what it should** + nothing more
- Should be **testable**: a 3rd party could determine whether requirement is met
- User stories:
  - brief description of single kind of interaction user can have with system
  - "As a *user* I can *action* so that *purpose*"
  - Examples from CMS:
    - As a professor, I can create a new assignment by specifying its name, number of possible points, and due date.
    - As a student, I can submit a file as a solution to an assignment.
- These stories reveal system assets

2. Threat analysis

- Identify threats of concern to system
  - Especially malicious, human threats
  - What kinds of attackers will system resist?
  - What are their motivations, resources, and capabilities?
- Best if analysis is specific to system and its functionality
- Non threats?
  - Trusted hardware
  - Trusted environment
  - e.g., physically secured machine room reachable only by trustworthy system operators

3. Harm analysis

- Harm: action adversely affects value of asset
- Harm to...
  - confidentiality: disclosure
  - integrity: modification or fabrication
  - availability: deprivation
- "Performing *action* on/to/with *asset* could cause *harm*"
  - e.g., "stealing money could cause loss of revenue"
  - e.g., "erasing account balances could cause loss of customers"

Harm triples

- <action, asset, harm>
  - e.g., <theft, money, loss of revenue>
  - e.g., <erasure, account balance, loss of customer>
- Useful methodology:
  - start with asset
  - brainstorm actions that could harm asset
  - let brainstorming be guided by CIA triad

Ex: GMS

- **Grade Management System:** manages just the final grade for a single course
- **Asset:** a numeric score for each student

Ex: GMS

Functional requirements:

- As a student, I can view my final grade.
- As a professor, I can view and change final grades for all students.
- As an administrator, I can add/remove students and professors to/from the course

Ex: GMS

Threat analysis:

- Students:
  - Motivations: increase their own grade, lower others' grades, learn others' grades
  - Capabilities: network access to servers, some physical access to others' computers, social engineering; probably not extensive computational or financial resources
- Out of scope: assume that threats cannot physically access any servers, profs are trusted, system admins

Ex: GMS

- **Asset:** a numeric score for each student
- **Functional requirements:** students view grades, profs view and change grades, admins manage enrollment
- **Threat analysis:** students might be malicious or curious; profs are trusted; threats can't access servers physically
- **Harm analysis:** performing *action* on/to/with *asset* could cause *harm*
- **Exercise:** invent some harm triples *<action, asset, harm>*

4. Security goals

- "The system shall prevent/detect *action* on/to/with *asset*."
  - e.g., "The system shall prevent theft of money"
  - e.g., "The system shall prevent erasure of account balances"
- Specify **what** not **how**
- Poor goals:
  - "the system shall use encryption to prevent reading of messages"
  - "the system shall use authentication to verify user identities"
  - "the system shall resist attacks"

Ex: GMS

Exercise: transform harm triples

<action, asset, harm>

into security goals

the system shall prevent/detect
action *on/to/with* asset

5. Feasibility analysis

- Not all goals are feasible to achieve
- Relax goals:
  - "prevent theft of items from a vault"
  - to "resist penetration for 30 minutes"
  - or to "detect theft of items from a vault"

From goals to requirements

- Goals: what should never happen in any situation
  - not testable
- Requirements: what should happen in specific situations
  - testable

6. Security requirements

- Constraints on functional requirements, in service of security goals
- Example:
  - **Functional requirement:** allow people to cash checks
  - **Security goal:** prevent loss of revenue through bad checks
  - **Security requirement:** check must be drawn on bank where it's being cashed (so funds can be verified), or customer must be account holder at bank and depositing funds in account (so funds could be reversed)

Security requirements

- Constraints on functional requirements, in service of security goals
- Another example:
  - **Functional requirement:** allow two users to chat using IM
  - **Security goal:** prevent disclosure of message contents to other users
  - **(Poor) security requirement:** contents of message cannot be read by anyone other than the two users
  - **(Improved) security requirement:** message is encrypted by key shared with the two users
    - doesn't over-commit to encryption algorithm, key size, etc.

Goals vs. requirements

Goals	Requirements
Broad scope	Narrow scope
Apply to system	Apply to individual functional requirements
State desires	State constraints
Not testable	Testable
Not about design/implementation details	Provide some details

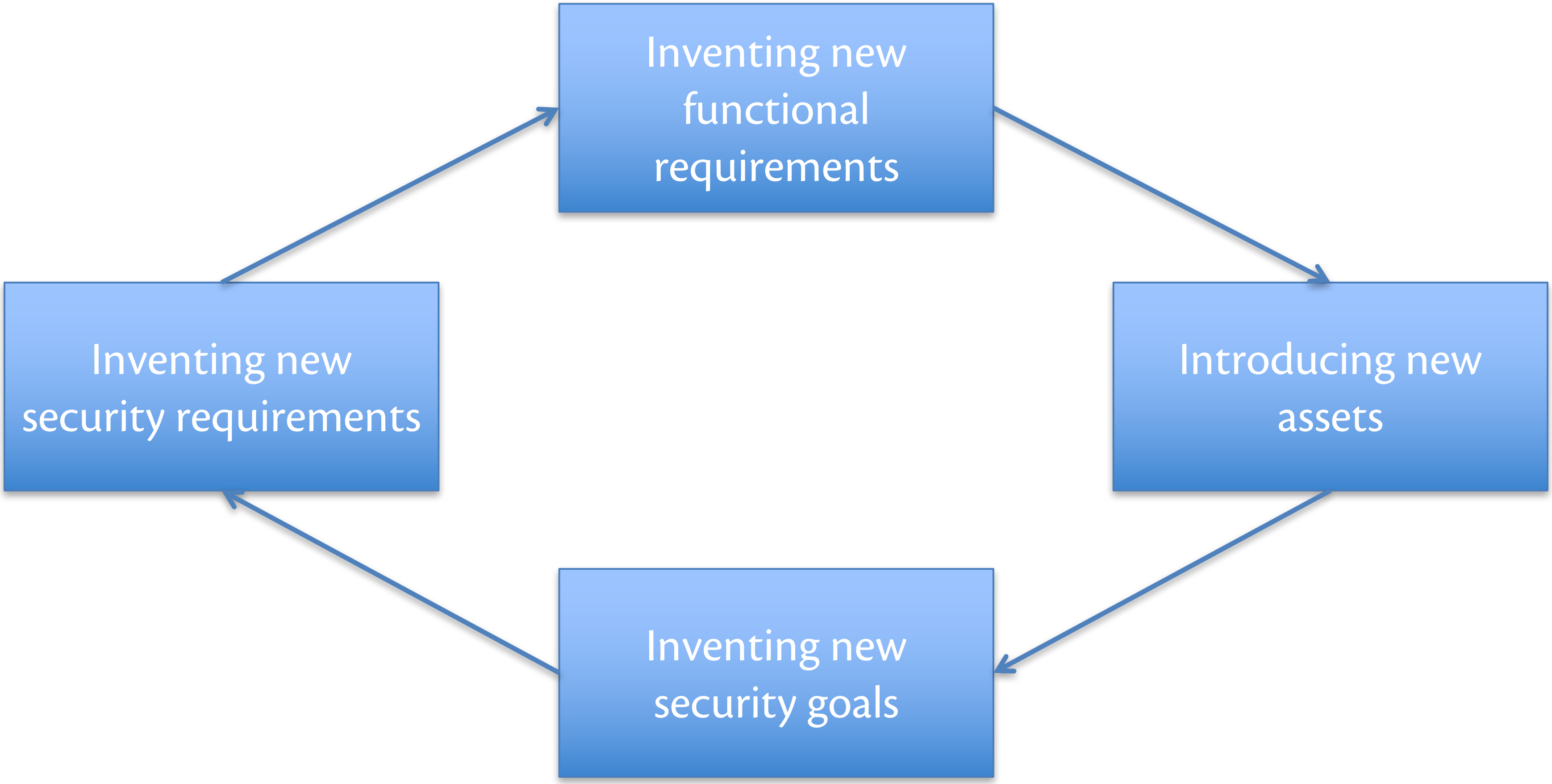
Ex: GMS

- **Functional requirements:** students view grades, profs view and change grades, admins manage enrollment
- **Security goals:** …
- **Security requirements:** *combine functional requirements with goals to invent constraints on system*

Engineering methodology

1. Functional requirements
2. Threat analysis
3. Harm analysis
4. Security goals
5. Feasibility analysis
6. Security requirements

Iteration



Inventing new functional requirements

Introducing new assets

Inventing new security goals

Inventing new security requirements

Upcoming events

- [Wed] Add deadline; everyone from waitlist should have PIN
  - Problems? See Megan Gatch in Student Services on first floor of Gates
- [next Wed] A1 due

"A desire presupposes the possibility of action to achieve it; action presupposes a goal that is worth achieving." – Ayn Rand